

CONTINUATION OF APPLICATION FOR SEARCH WARRANT

I. APPLICANT INFORMATION

1. I, Timothy Kruithoff, have been employed as a Special Agent with the Department of Homeland Security Investigations (HSI) since August 2002. Prior to becoming a Special Agent, I was employed as U.S. Customs Inspector. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the sexual exploitation of children (i.e. production of child pornography), in violation of 18 U.S.C. § 2251(a) and violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a). I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in many forms of media, including computer media.

2. This continuation is based on my training, knowledge, education, and experience in the investigation of violations of federal criminal laws, my conversations with witnesses and other law enforcement officers, my review of relevant documents, and my personal observations. Because it is submitted for the limited purpose of establishing probable cause to search for evidence, this summary does not necessarily recite all of the facts of the underlying investigation that are known to me or to other investigators at this time. For the reasons I explain in this continuation, I submit there is probable cause to believe that property will be found at the place to be searched, and that this property will constitute evidence of the criminal violations of the following statutes: 18 U.S.C. § 2251(a) - Sexual Exploitation of Children (i.e. production of child pornography); 18 U.S.C. §§ 2252A(a)(2) (distribution or receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography). The property I am seeking authorization to search and seize includes information (consistent with Fed. R. Crim. P. 41(a)(2)(A)) and is as described particularly in Attachment "B" to the Search Warrant Application

3. I am advised by the United States Attorney's Office that, per 18 U.S.C. § 2256(8)(a), "child pornography" means "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct[.]"

4. I am currently investigating WESTLEY JAMES KEYES, a 39-year-old man who maintains an address at 168 Thelma Drive, Emmet Township (Battle Creek), Michigan, the "SUBJECT PREMISES".

- a. In September of 2021 Homeland Security Investigations (HSI) Grand Rapids received information from the HSI Cyber Crime Center (C3) Child Exploitation Investigations Unit (CEIU) Victim Identification Program/Lab team in regards to a lead from the Queensland Police Service (QPS) Child Abuse & Sexual Crime Group Task Force ARGOS, consisting of current

and former Law Enforcement personnel, regarding forty two (42) child abuse images and fourteen (14) non-abuse images first shared by the Tor user/profile 'hotlips666' on a dark web child exploitation chat site/forum from May of 2020. Some of the images were found to have had EXIF data embedded within the images.

- b. Investigators used the EXIF data (EXIF stands for Exchangeable Image File Format and refers to the basic metadata that is generated and stored by a camera when taking an image) to identify a female teenager (Minor 1) depicted in non-abuse images. A forensic interview of Minor 1 was conducted on January 10, 2022. During the interview Minor 1 provided information which identified KEYES as the only individual who could have taken one of the non-abuse images of her.
- c. At the time of the forensic interview, Minor 1's mother told investigators that her brother JM has a young daughter aged 5 or 6 years. Investigators went to JM's home and met with JM's wife, KM, who confirmed that Minor 2, a female toddler depicted in abuse images with EXIF data, is her daughter. The abuse images of Minor 2 contain the same EXIF data as Minor 1's non-abuse photographs.
- d. WESLEY received a conviction for Child Sexually Abusive Activity – Distributing or Promoting in 2016.
- e. Additionally on January 10, 2022, HSI Grand Rapids Special Agents went to SUBJECT PREMISES and encountered WESTLEY JAMES KEYES. After securing the residence and later learning Minor 2 disclosed that KEYES pulled her underwear down and took pictures of her genitalia, KEYES was arrested on probable cause. KEYES was read his Miranda Warning and he consented to HSI Special Agents searching his bedroom.
- f. I am seeking authorization to search the electronic items seized from KEYES bedroom specified in Attachment A. There is probable cause that KEYES has produced child pornography, in violation of 18 U.S.C. § 2251(a) and that KEYES has distributed or received of child pornography and possessed child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and (a)(5)(b).

II. JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States.... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

III. PROBABLE CAUSE

6. In September of 2021 Homeland Security Investigations (HSI) Grand Rapids received information from the HSI Cyber Crime Center (C3) Child Exploitation Investigations Unit (CEIU) Victim Identification Program/Lab team in regards to a lead from the Queensland Police Service (QPS) Child Abuse & Sexual Crime Group Task Force ARGOS, consisting of current and former Law Enforcement personnel, regarding forty two (42) child abuse images and fourteen (14) non-abuse images first shared by the Tor user/profile 'hotlips666' on a dark web child exploitation chat site/forum from May of 2020.

7. Queensland Police Service is actively investigating darknet boards that are known to be dedicated to the proliferation of child exploitation material. During its investigation, Queensland Police Service saw imagery posted by "Hotlips666" and sought to identify the location depicted in the imagery.

- a. During Queensland Police Service's review of the non-abuse image, 89565549948.jpg, which depicts a pre-pubescent female wearing a bathing suit and standing on an informational panel next to a river/creek, Queensland Police Service ARGOS identified the outside location as the Historic Bridge Park in Battle Creek, Michigan.
- b. During Queensland Police Service ARGOS review of another non-abuse image, 565808938.jpg, which depicts the same child in a different location in a park setting. She is wearing a different bathing suit while laying on a picnic bench. Queensland Police Service ARGOS identified the outside location as the Ross Township Park, Hickory Corners, MI 49060.
- c. During Queensland Police Service ARGOS review of another non-abuse image, 565965000.jpg, which depicts the same child in residential area, Queensland Police Service ARGOS identified the outside location as being in front of the address 109 Hwy St, Battle Creek, Michigan. These locations were identified by Queensland Police Service ARGOS using manual man hours surfing open-source images and street-views of locations.

8. In addition to Queensland Police Service ARGOS identification of several of these images posted being taken in the Battle Creek, Michigan area, several other images posted by "Hotlips666" and provided to HSI Grand Rapids, were found to have had EXIF data embedded within the images.

- a. EXIF stands for Exchangeable Image File Format and refers to the basic metadata that is generated and stored by a camera when taking an image. EXIF data may include identification of the device used to capture the image, the date and time the image was captured, as well as the GPS location.
- b. This EXIF data, in some of the abuse and non-abuse images provided to HIS Grand Rapids show the images were taken with a Samsung phone, model #SM-G973U1 in June and August 2020.

- c. There are two minors depicted separately in multiple images with EXIF data: a female teenager and a female aged approximately 2-4 years.

9. Law enforcement identified a female teenager (Minor 1) depicted in several of the non-abuse images with EXIF data.

10. On January 10, 2022, Minor 1 was forensically interviewed by Homeland Security Interview Specialist Amy Allen. The following is information obtained from that interview:

- a. Minor 1 was shown 4 images. Minor 1 identified the location depicted in all four photographs as her grandparents' home, the SUBJECT PREMISES.
 - i. Minor 1 stated the photographs were taken during a family reunion which took place at the SUBJECT PREMISES. Minor 1 stated that she was certain as to when the photographs were taken because she had her nails done specifically for this event.
 - ii. It should be noted that 1 image depicts Minor 1's manicure clearly: false nails applied to each nail with alternating colors of white and green (i.e. every other nail painted is painted green).
- b. The focus of one of the images is Minor 1's genital area. Minor 1 stated that she is sitting on a bench in the SUBJECT PREMISES' backyard in that image. The bench runs along a deck at ground level. Minor 1 recalled that when she was seated on the bench her two uncles, KEYES and MM, were in the immediate area. Minor 1 stated other people were also outside, but they were up on the deck. Minor 1 stated that her minor brother was also outside in the grass during this time, but he did not have a phone.
- c. Minor 1 described where MM and KEYES were seated/standing during their conversation at the bench. Based on that description, KEYES was in a position to take the image of Minor 1 seated on the bench, but MM was not.

11. Following the forensic interview, I spoke with Minor 1's mother. Minor 1's mother stated that she is aware that KEYES had previously been convicted of a crime involving child pornography. Minor 1's mother stated that her brother JM shared concerns with her regarding his observation of KEYES taking photographs of children at times which did not seem appropriate such as during a diaper change. Minor 1's mother stated her brother JM is married to KM and they have a female child whom she believes is currently 5 or 6 years of age. Minor 1's mother stated that KEYES currently resides at "SUBJECT PREMISES" with KEYES' grandparents, JK and RK.

12. On January 10, 2022, investigators went to JM and KM's home. KM was home at the time and agreed to speak with investigators. Investigators showed KM sanitized versions of abuse images depicting Minor 2. KM confirmed that Minor 2 is her daughter. KM produced to investigators a pair of underpants depicted in one of the images. KM stated she is aware that KEYES has had a Samsung phone in the past because she previously considered purchasing it from KEYES.

13. Homeland Security Interview Specialist Amy Allen conducted a forensic interview of Minor 2. During the interview Minor 2 reported that KEYES took photographs of her genitalia.

14. Due to safety concerns for KEYES and to prevent the destruction of evidence, following KM's positive identification of Minor 2 on January 10, 2022, HSI Grand Rapids Special Agents went to the SUBJECT PREMISES to secure it and encountered KEYES, JK and RK.

15. JK and RK are KEYES' grandparents and own the SUBJECT PREMISES. JK and RK denied any knowledge of KEYES' producing and/or possessing child pornography. JK and RK provided consent to search the SUBJECT PREMISES. JK and RK stated KEYES resides downstairs in a bedroom inside the SUBJECT PREMISES. JK and RK, in summary, stated out of respect for KEYES' privacy they do not enter or use that space.

16. After securing the residence and later learning Minor 2 disclosed that KEYES pulled her underwear down and took pictures of her genitalia, KEYES was arrested on probable cause. KEYES was read his Miranda Warning and he consented to HSI Special Agents searching his bedroom.

17. During the search of KEYES' bedroom, investigators discovered the following electronic devices: Samsung Galaxy phone, model #SM-G973U1, IMEI #352338107385419; Toshiba Satellite laptop, S/N #9B276675K; Acer laptop Model #5315, S/N #81506623316; HP laptop Model #G60642NR, S/N#2CE01914SK; Omen laptop, Model #15-EN1013DX, S/N#5CD1238S46; Samsung portable SSD external hard drive, S/N #S5TFNJ0R103421A (collectively SUBJECT DEVICES).

18. KEYES refused to provide his fingerprint or other passwords in order to access the SUBJECT DEVICES.

19. A review of KEYES' criminal history revealed a 2016 conviction for Child Sexually Abusive Activity – Distributing or Promoting and an address of "168 Thelma, Battle Creek Michigan."

20. On January 11, 2022, following his initial court appearance in 1:22-MJ-00009, KEYES provided me with the passcode to his Samsung Galaxy phone. I successfully entered the passcode and placed the Samsung Galaxy in airplane mode.

21. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the distribution, receipt, and collection of child pornography. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person.

22. In this case, communications as described above took place in different dark web boards. Queensland Police Service provided HSI Grand Rapids with chat messages it obtained from different dark web boards posted by the user profile of "Hotlips666." Those messages include the following:

2020-04-04T20:25:58.100Z	i love them to be g 38 the for me
2020-04-04T20:26:24.100Z	3-8
2020-04-04T20:27:07.100Z	my bad all lmao
2020-04-22T13:06:52.000Z	Hi Im into girls 3-8 I am a single father and will do my best share what I have and I like to participate in chat rooms
2020-04-23T08:13:00.100Z	little girls are sooo hot
2020-04-23T08:21:00.100Z	I haven't been able to find any good hurtcore lately
2020-05-14T08:21:46.000Z	Is there anybody on here in to kill and little girls you so please PM me
2020-05-14T08:36:00.100Z	Lookin for somebody and to killing little girls please PM
2020-05-15T11:20:00.098Z	Man I love some good pussy
2020-05-15T12:14:56.000Z	Look I don't like asking but I just got out of president lost all my collection does anybody have links to neurology ty
2020-05-15T12:16:14.000Z	Prison
2020-05-15T13:10:46.000Z	love dead pussy all day
2020-05-15T13:50:00.100Z	I get to see my 3 yr niece today first time
2020-05-15T13:51:00.100Z	And my brother is going to let me have her overnight so I'm so excited right now
2020-05-15T13:53:00.096Z	I will be putting pic up later tonight
2020-05-15T13:56:00.092Z	She going to be a good CP star soon

2020-05-17T11:00:54.100Z	yes a lot of nice people on here and that's why I jut pictures of my daughter's on here
2020-05-17T11:11:29.100Z	I would seriously like it if somebody would kidnap her and one day find pictures of her on here so
2020-05-17T11:18:00.100Z	A few days ago a guy was showing me pictures of dead little girls and I can't stop thinking about them
2020-06-05T17:18:00.100Z	I love just think about what happens to these little girls that get kidnapped
2020-06-05T17:19:00.099Z	Most jelly time it doesn't in well and I know at least half of the pictures I can find are at least kidnapped kids so hot
2020-06-13T13:40:58.000Z	I would love to watch somebody snuff my daughter in front of me
2020-06-13T13:44:45.000Z	she's 7
2020-06-17T14:23:00.100Z	I would love to watch what would happen if I left my 8 year old daughter in a Room with all of you
2020-06-17T14:28:00.097Z	So hot
2020-06-17T14:36:00.100Z	I let her sleep out side in hopes someone will kidnap her
2020-06-17T14:42:00.097Z	I hop you all like please pass her around
2020-06-17T14:43:00.100Z	I promise if I see her passed around on here I will put more of her on here maybe even take request
2020-06-17T14:43:00.100Z	Trying to make her in to a CP star
2020-06-17T14:45:00.097Z	I'd love for all of you to give her some pedo dick
2020-06-17T14:46:00.098Z	I'm just trying to pay it forward
2020-06-17T14:47:00.098Z	No I'm not in to fucking my kid but I'll let others at her
2020-06-17T14:47:00.100Z	I'd love it if you rape her
2020-06-17T14:48:00.099Z	6
2020-07-06T12:40:59.000Z	I'd love to have my niece to fuck a pig

2020-12-07T10:02:00.100Z	God i love being a pedo
2020-12-07T10:04:00.097Z	To all LEA on here tonight I kidnapped my first sex toy
2020-12-07T10:04:00.098Z	I will post the pictures soon she was a good fuck
2020-12-07T10:08:00.100Z	most LEA love looking at CP and get paid for it
2020-12-07T10:09:00.100Z	is BS
2020-12-07T10:09:00.100Z	look on here they post pictures of kids get fuck and that
2020-12-07T10:14:00.099Z	she was 7
2020-12-07T11:03:00.100Z	does any one have necro or snuff link if so ty

23. I reviewed the chat logs and identified the image (1eemq4jhe.jpg) that was sent on 08-02-2020, as a non-abuse image with EXIF data depicting Minor 1. The EXIF data in “1eemq4jhe.jpg” matches EXIF data in the abuse and non-abuse images depicting Minor 2. The following are the chat messages:

2020-08-02T05:21:56.100Z	my lovers
2020-08-02T05:26:46.100Z	g. http://oju4yn237c6hjh42qothvpreqecnjhtvh4sgn3fqmsdvhu5d5tyspid.onion/i/1eemq4jhe.jpg

24. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, individuals may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Evidence of this activity—including some or all of the child pornography files themselves—would likely be located on the computer from which the individual accessed the URL and the chat room and evidence of that activity can be forensically recovered from the computer.

IV. SPECIFICS OF SEIZING AND SEARCHING COMPUTER SYSTEMS

25. Computers and Internet-capable devices such as tablets and cellular telephones facilitate the collection and distribution of child pornography. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

26. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously in recent years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files, including images, video files, and full-length movie files.

27. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

28. A forensic examiner often can recover evidence that shows whether a computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

29. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file often does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

30. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

31. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

32. In order to retrieve data fully from a computer system, the analyst needs all storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

33. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

34. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The Government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of

irrelevant materials.

VI. REQUEST FOR SEALING

35. I respectfully request that the Court issue an order sealing, until further order of this Court, all papers submitted in support of this application, including the application, continuation, attachments, and search warrant, and the requisite inventory notice. I believe sealing is necessary because premature disclosure of the contents of this continuation and related documents may jeopardize this continuing investigation by alerting the target and providing an opportunity to destroy evidence.

VII. CONCLUSION

36. I respectfully submit that there is probable cause to believe that WESTLEY JAMES KEYES, an individual who resides at 168 Thelma Drive, Emmet Township (Battle Creek), Michigan, is involved in the criminal violations of the following statutes: 18 U.S.C. § 2251(a) - Sexual Exploitation of Children (i.e. production of child pornography); 18 U.S.C. §§ 2252A(a)(2) (distribution or receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography), and that evidence, fruits, and instrumentalities of those crimes are contained in the SUBJECT DEVICES listed in Attachment A.

37. Because there is probable cause that evidence of the above offenses is located on the SUBJECT DEVICES seized from the SUBJECT PREMISES, I respectfully request that the Court issue a search warrant that would allow agents to search the electronic items seized as evidence from 168 Thelma Drive, Emmet Township (Battle Creek), Michigan. The items and information sought to be seized are more specifically described in Attachment B.